apdcat
Autoritat Catalana de Protecció de Dades

Recomendación 1/2013

de la Autoridad Catalana de Protección de Datos, sobre el uso del correo electrónico en el ámbito laboral

Generalitat de Catalunya

Introducción

El uso de las tecnologías de la información y la comunicación en la actividad de las administraciones públicas, y entre ellas el uso de sistemas de correo electrónico, ha comportado, sin ningún tipo de duda, un gran avance en la eficacia de la actividad del sector público. La inmediatez de la comunicación, el gran volumen de información que puede circular por la red, la posibilidad de acceder a la información desde fuera del puesto de trabajo y la reducción de costes ligada a la utilización de un sistema de correo electrónico han hecho de esta herramienta un elemento imprescindible en cualquier organización administrativa. Pero los innegables aspectos positivos que incorpora el uso de estas tecnologías no permiten infravalorar los riesgos derivados del uso del correo electrónico para la seguridad de la información y la protección de los datos de carácter personal.

De acuerdo con lo que establece el artículo 8.2.e) de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, corresponde a la directora de la Autoridad dictar las instrucciones y las recomendaciones necesarias para adecuar los tratamientos de datos personales a los principios de la legislación vigente en materia de datos de carácter personal. Por ello, resulta conveniente ofrecer pautas y buenas prácticas en el uso de estos sistemas de comunicación mediante una Recomendación.

Esta Recomendación se dirige a las administraciones públicas catalanas, y también a todos los otros entes incluidos dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos. Con independencia de su naturaleza pública o privada, y con independencia también de la naturaleza del vínculo jurídico que establezcan con sus trabajadores, estos entes adoptan la posición jurídica del empresario. Es por ello que, en esta Recomendación, nos referiremos a todos estos entes bajo la denominación *empresa*.

La Recomendación se dirige, especialmente, a los responsables de la información, a los responsables de seguridad y a las personas trabajadoras de estas entidades, que tienen encomendadas tareas en relación con la configuración de los sistemas de tecnologías de la información y la comunicación, y sobre la seguridad de la información en la empresa, con la voluntad de ser una herramienta para la reflexión previa a la toma de decisiones corporativas en este ámbito.

Esta Recomendación se complementa con el *Manual del buen uso del correo electrónico*, que se publica de forma simultánea con esta Recomendación. El manual, que podréis encontrar en la web de la Autoridad y que os podréis descargar, se dirige a todas las personas trabajadoras de estas entidades que tienen que utilizar el correo electrónico para ejercer sus funciones, a fin de que en su uso adopten prácticas que garanticen el tratamiento adecuado de su propia información personal, como también de la privacidad de terceras personas.

El objeto de esta Recomendación, que no tiene carácter normativo, es precisamente, dar pautas para que las empresas puedan regular y controlar el uso del correo electrónico en el ámbito laboral. Por eso, en ella se incluyen recomendaciones que puedan ayudar a difundir buenas prácticas y que contribuyan a ofrecer más seguridad y más respeto por los derechos de las personas, en especial por el derecho a la protección de los datos de carácter personal.

Y ello cada organización lo tiene que hacer de acuerdo con sus necesidades en el momento de tratar la información de la cual es responsable. En esta tarea tiene un papel fundamental la aprobación de unas normas de uso del correo electrónico.

En cualquier caso, visto el carácter cambiante de la tecnología y, en consecuencia, de la materia objeto de esta iniciativa, la presente Recomendación no se concibe como algo estático, sino más bien como una herramienta dinámica, la aplicación de la cual estará sometida, por parte de la misma Autoridad Catalana de Protección de Datos, a un proceso continuado de verificación para comprobar los resultados de su aplicación y adecuar las previsiones que en ella se contienen a los nuevos problemas que se puedan plantear.

I. El correo electrónico

1 Sistemas de correo electrónico

El correo electrónico es un sistema de mensajería que permite la transmisión de mensajes entre usuarios sin necesidad que estén conectados al mismo tiempo. Hay diferentes aplicaciones que permiten gestionar los mensajes de correo electrónico, que se pueden agrupar, básicamente, en dos modalidades:

❑ Cliente de correo electrónico

Son programas (p. ej. Outlook, Outlook Express, Eudora, Mozilla Thunderbird, etc.) que sirven para gestionar los mensajes recibidos y para escribir nuevos mensajes. El programa descarga todos los mensajes que se almacenan en el ordenador, sin perjuicio que determinados protocolos (caso de IMAP) puedan mantenerlos en el servidor. Se puede instalar en diferentes dispositivos (ordenador fijo, portátil, teléfono inteligente o *smartphone*, tableta, etc...).

❑ Webmail o correo web

Hay sistemas de correo que se identifican habitualmente como correo web o web mail. Con independencia que se pueda acceder a él también a través de un cliente de correo, se trata de un sistema de acceso a un servicio de correo electrónico utilizando el navegador de Internet y el protocolo http o https. Este sistema permite recibir y enviar correos desde cualquier lugar, a través de una web. Los mensajes se almacenan en el servidor donde se aloja la cuenta de correo.

Los servidores de correo web pueden estar en terceros países, que quizás no cuentan con un nivel adecuado de protección de los datos de carácter personal y, especialmente en el caso del web mail, a menudo las condiciones las fija y las modifica unilateralmente el proveedor. Si se trata de servicios ofrecidos gratuitamente, estas condiciones a menudo incluyen la autorización para el tratamiento de la información que contienen, con finalidades publicitarias u otras finalidades. A menudo, también realizan un análisis automático del contenido de los mensajes enviados o recibidos. Este análisis del contenido de los mensajes puede ser útil, por ejemplo para detectar virus, pero hay que advertir que los proveedores también lo pueden utilizar para ofrecer, en la misma aplicación de correo, anuncios que estén relacionados con dicho contenido.

Recomendaciones

- ✓ Atribuir una cuenta de correo a los trabajadores que lo necesiten para ejercer sus funciones, ya sea mediante el sistema de cliente de correo electrónico o de correo web. En este último caso, conviene asegurar que la empresa que facilita el correo tenga establecidas políticas de privacidad y seguridad adecuadas, a través de las correspondientes cláusulas contractuales vinculantes para todas las partes implicadas.

2 La dirección de correo electrónico

2.1 La dirección de correo electrónico como dato personal

La dirección de correo electrónico es el conjunto de palabras o signos que identifican el emisor o el receptor de un mensaje de correo electrónico. Se elabora a partir de un conjunto de palabras o signos libremente escogidos, normalmente por su titular o por la organización a la cual pertenece, con el único límite de que esta dirección no coincida con la de otra persona. Está formada por una identificación del usuario, seguido del signo @ y, a continuación, el dominio (identificación facilitada por el proveedor del servicio de correo, con un punto, y unas siglas que pueden identificar la actividad de la organización (p. ej. ".org") o las siglas del país (p. ex. ".es" o ".cat").

Se puede distinguir:

❑ Direcciones personalizadas

La dirección contiene directamente información sobre su titular: nombre y apellidos, iniciales, cargo, número identificativo, etc.

- ✓ Nombre_Apellidos_@nombre_del_dominio
  joanidentitat@gencat.cat
- ✓ Iniciales_@nombre_del_dominio
  E.C@gencat.cat
- ✓ Cargo@nombre_del_dominio
  Directoraautoridad@gencat.cat
- ✓ Número identificativo@nombre_del_dominio
  000000000857346@gencat.cat

En estos casos, la dirección de correo electrónico identifica directamente al titular de la cuenta y por lo tanto hay que considerarlo como dato de carácter personal.

La atribución de una dirección de correo de este tipo puede generar falsas expectativas de privacidad, tanto a la persona titular como a las personas que se relacionan con ella. Por ello, en los casos en que se quiera prohibir totalmente la utilización del correo con fines personales, puede no ser conveniente atribuir una dirección de correo personalizada.

❑ Direcciones no personalizadas

Aunque se trata de una dirección vinculada a una cuenta de correo de una persona física determinada, la dirección de correo electrónico no parece contener información sobre su titular (utiliza una combinación alfanumérica abstracta o sin ningún significado):

Akatombe80@gmail.com

Abc123@terra.net

En estos casos, la dirección por sí sola no identifica a la persona que es titular de la misma. Pero ésta puede ser fácilmente identificable sin un esfuerzo desproporcionado, bien porque la dirección puede aparecer junto con otros datos que permiten su identificación, bien por el contenido del mensaje, bien a través de los datos que dispone el servidor de correo. Esta dirección también hay que considerarla como dato de carácter personal.

❑ Direcciones genéricas

La dirección de correo electrónico responde a una cuenta genérica, de uso compartido o de un área de la organización:

consultas@gencat.cat

En estos casos, la dirección de correo electrónico no se puede vincular a una persona física identificada o identificable, sino que la pueden atender diferentes usuarios. Por lo tanto, no se puede considerar como dato de carácter personal. Con una dirección de este tipo desaparecen las expectativas de privacidad tanto del mismo trabajador como, especialmente, de las personas que se relacionan con él, dado que esta cuenta de correo puede ser atendida por diferentes usuarios.

2.2 Publicación de la dirección de correo electrónico en Internet/ Intranet como dato de contacto

La publicación de la dirección de correo laboral o profesional que se pueda asociar a personas físicas constituye una comunicación de datos de carácter personal y, por lo tanto, tiene que sujetarse al régimen de comunicaciones previsto en la normativa de protección de datos. Ello quiere decir que es necesario disponer del consentimiento de la persona trabajadora o de una norma con rango de ley que habilite su comunicación.

En la medida en que la publicación de la dirección de correo electrónico laboral o profesional sea necesaria como parte del desarrollo de las funciones que puede tener atribuidas un determinado puesto de trabajo, su difusión debe considerarse amparada en el artículo 6.2 y 11.2.c) de la LOPD y en el artículo 2.2 del RLOPD.

Por otra parte, en el caso de las listas de personas pertenecientes a grupos de profesionales, que tienen la consideración de fuentes de acceso público de acuerdo con los artículos 3. j) de la LOPD y 7 del RLOPD, la dirección electrónica, que forma parte de los datos incluidos en esta fuente de acceso público, se puede tratar para la satisfacción de un interés legítimo perseguido por el responsable del fichero o por el tercero a quien se comunique este dato, siempre que no se vulneren los derechos y libertades fundamentales de la persona afectada (art. 6.2 LOPD).

Recomendaciones

- ✓ Establecer cuentas de correo vinculadas a trámites, servicios o áreas de actividad, en lugar de personas determinadas, siempre que sea posible. Esto puede ser especialmente recomendable cuando se facilitan cuentas de correo a trabajadores de empresas externas que prestan servicios de forma habitual dentro de la empresa.
- ✓ Limitar la difusión de la dirección electrónica de las personas trabajadoras a aquellos supuestos en que resulte necesario para las funciones atribuidas a cada una de ellas. En el resto de supuestos, publicar la dirección de correo electrónico sólo en la Intranet.
- ✓ Incorporar en el lugar donde se difundan las direcciones, un recordatorio de los usos admitidos de estas direcciones.
- ✓ Incorporar mecanismos para evitar la indexación de las direcciones de correo, cuando se publiquen en la web, para evitar que se puedan utilizar para envíos masivos de correos electrónicos. En este sentido, puede ser recomendable no incluir en la visualización de las páginas la dirección de correo, sino sólo un enlace que, al hacer clic en él, sí que permita acceder a una página que incorpora una instrucción de no indexación, que contiene la dirección. De esta manera se puede permitir indexar el contenido de la página inicial que contiene el enlace, sin indexar la dirección.
- ✓ No utilizar, ni ceder a terceras personas, las direcciones de correo que forman parte del directorio corporativo, para finalidades diferentes de aquéllas que resulten necesarias para desarrollar las funciones encomendadas a la empresa.

3 El contenido del correo electrónico

En un correo electrónico figura diversa información que se puede considerar como dato de carácter personal, en la medida en que nos ofrezca información sobre una persona física identificable:

❑ Dirección de correo del emisor y el destinatario o destinatarios

La dirección de correo se puede vincular fácilmente a una persona física. En ocasiones, la misma dirección ya facilita su identificación. En otros casos, en el campo correspondiente a la dirección, junto con ella, o incluso sustituyéndola, aparece la identificación de la persona que es su titular.

❑ Asunto sobre el cual versa el correo

Conviene que el asunto describa de forma concisa la naturaleza o el contenido del mensaje y, si es posible, se evite incluir en él datos de carácter personal.

El grado de confidencialidad de los datos que se incluyan en él será menor que el de la información que contiene el cuerpo del mensaje, dado que la simple visualización de la bandeja de entrada o salida permite leer el asunto.

❑ Fecha y hora del correo

La fecha y la hora del correo también constituyen un dato personal, dado que permiten establecer el momento en que se envía e, incluso, pueden llegar a permitir establecer el lugar donde estaba una persona.

❑ Cuerpo del mensaje

Es el contenido del mensaje. Puede consistir en un texto, con formato o sin, o en imágenes, que pueden contener datos de carácter personal. También puede contener enlaces a páginas web o documentos que contengan datos personales.

❑ Pie de firma

Es el texto que aparece debajo de la identificación de quién suscribe el mensaje. Normalmente, ofrece información sobre el cargo y la organización a la cual pertenece el emisor.

A menudo, los sistemas de correo electrónico ofrecen la posibilidad de incorporar en los mensajes de correo un pie de firma de forma automática.

❑ Documentos adjuntos

El correo electrónico permite adjuntar al mensaje imágenes, documentos, vídeos o audio. El volumen de información personal que pueden incluir los documentos adjuntos puede ser muy grande, por lo cual, para evitar revelaciones indebidas de información, conviene extremar la prudencia cuando se adjunten ficheros. Además, hay que velar por la seguridad de estos datos y, si procede, valorar el uso de medios técnicos, como técnicas de cifrado, para asegurar que el contenido no será interceptado por terceros.

II. El uso del correo electrónico

1 Normas de uso del correo electrónico

Con el fin de evitar una mala utilización del correo electrónico que pueda perjudicar la seguridad de la información de la que se trata, la empresa tiene que establecer y poner en conocimiento de sus trabajadores las normas de uso del correo electrónico y definir las condiciones en que, si procede, esta herramienta se puede utilizar con finalidades privadas.

El establecimiento, mediante estas normas, de una política de uso del correo tiene que permitir a las personas trabajadoras conocer con seguridad el nivel de confidencialidad que pueden esperar en el uso de estas tecnologías. La falta de una política adecuada de uso del correo electrónico, en cambio, puede producir, en la persona trabajadora o en terceros, una expectativa de confidencialidad que puede dar lugar a situaciones conflictivas.

En su elaboración, conviene contar, siempre que sea posible, con la participación de los representantes de las personas trabajadoras.

Se tiene que informar a las personas trabajadoras de la existencia de estas normas. Aparte de hacer difusión de ellas en la intranet de la empresa, para garantizar que todas las personas trabajadoras las conozcan, se pueden incorporar, como anexo, a los contratos laborales, pueden formar parte del manual de bienvenida o pueden adoptar la forma de circulares o instrucciones comunicadas a los trabajadores.

Aparte de su participación en la elaboración de estas normas, también conviene informar a los representantes de las personas trabajadoras de las normas que se aprueben.

La empresa tiene que formar a sus trabajadores en el uso del correo electrónico y, especialmente, en el conocimiento de las opciones de privacidad que ofrezca el sistema utilizado por la empresa.

Estas normas se tienen que actualizar de acuerdo con la evolución de la tecnología disponible, de la actividad de la empresa y de las necesidades de las personas trabajadoras.

En estas normas se tendrían que tratar, como mínimo, los aspectos siguientes:

- ❑ Objeto y finalidad del documento.
- ❑ Especificaciones del sistema de correo electrónico (equipos y software).
- ❑ Instrucciones generales de uso del correo electrónico.
- ❑ Usos admitidos y usos no admitidos del correo electrónico profesional y, si procede, de la cuenta de correo personal facilitada por la empresa. En caso de admitirse un cierto uso privado, conviene determinar las condiciones de este uso (grado de utilización con finalidades privadas, identificación de los mensajes privados, almacenaje, eliminación del pie de firma en los mensajes privados, etc.).

- ❑ Usos admitidos de los soportes y dispositivos móviles o portátiles facilitados por la empresa que permitan acceder al correo electrónico.
- ❑ Posibilidad o no de utilizar sistemas de correo web en el puesto de trabajo, ya sea con finalidades profesionales o estrictamente personales, o de recibir en la cuenta cliente corporativa mensajes de otras cuentas.
- ❑ Aspectos relativos al contenido de los mensajes: encabezamientos, aspectos formales, lenguaje, avisos legales, pies de firma, medida máxima de los archivos, etc.
- ❑ Usos admitidos de las direcciones publicadas en el directorio de la empresa.
- ❑ Medidas de seguridad aplicables:
  - Medidas de identificación y autenticación de usuarios: asignación de claves y política de contraseñas.
  - Medidas que tienen que adoptar las personas trabajadoras para garantizar la confidencialidad de la información y, si procede, el secreto profesional.
  - Procedimiento para autorizar la transmisión de datos a través de la red.
  - Utilización de la firma electrónica y mecanismos de cifrado.
  - Protocolo a seguir por las personas trabajadoras, y por la misma empresa, en caso de que se produzca alguna incidencia en el uso del correo.
  - Otras medidas de seguridad.
- ❑ Periodos de conservación de la información en las carpetas de entrada, de elementos enviados y en la papelera, en sistemas de cliente de correo.
- ❑ Informaciones que se tienen que conservar durante un periodo más largo en forma centralizada o bien, por ejemplo, en copias de seguridad, para la gestión técnica de la red o archivos "log".
- ❑ Soluciones para garantizar la continuidad de la actividad en caso de ausencia de la persona trabajadora, con especial referencia a los mensajes de respuesta automática.
- ❑ Tratamiento que hay que dar a los mensajes inadecuados que se reciban.
- ❑ Medidas de control del uso de correo que puede llevar a cabo la empresa:
  - Mecanismos de filtrado.
  - Programas y dispositivos de control y monitorización, si están justificados.
  - Supuestos y procedimiento de acceso a las cuentas de correo por parte de la empresa.
- ❑ Consecuencias para la persona trabajadora del uso indebido del correo electrónico.
- ❑ Otras normas de buen uso del correo electrónico dirigidas a las personas trabajadoras o normas de comportamiento general en la red o *netiquettes*. Con esta finalidad, esta Autoridad ha publicado también el *Manual del buen uso del correo electrónico*, dirigido específicamente a los trabajadores usuarios de los sistemas de correo electrónico.

En el Anexo I de esta Recomendación se ofrece un modelo de normas de uso del correo electrónico en el ámbito laboral, que se puede utilizar para elaborar las normas de cada empresa. Conviene adecuar este modelo a las necesidades de cada organización, respecto al tratamiento de la información.

2 Los mecanismos de identificación y autenticación

❑ Identificación

Procedimiento para conocer la identidad de un usuario, en este caso del usuario de correo electrónico. Con esta finalidad, se asigna un nombre a cada usuario.

❑ Autenticación

Procedimiento de comprobación de la identidad de un usuario. En un sistema de correo, esto se hace normalmente a través de la introducción de una contraseña o *password* además de la identificación del usuario, aunque también se pueden utilizar otros sistemas, como un certificado digital.

❑ Contraseña

Información confidencial, constituida por una cadena de caracteres. La robustez de esta contraseña depende de las características exigidas para establecerla (política de contraseñas). Una contraseña se puede considerar fuerte si:

- Tiene una longitud mínima de 8 caracteres.
- Se ha escogido al azar y no se puede encontrar en ningún diccionario.
- Sólo la puede deducir el mismo usuario.
- Requiere esfuerzos desproporcionados averiguarla.
- Incluye letras, números, mayúsculas y minúsculas y, si el sistema lo permite, símbolos.

En cambio, se puede considerar que una contraseña es débil si:

- Identifica fácilmente al usuario.
- Contiene menos de 8 caracteres.
- Viene predeterminada por el sistema o por el administrador del sistema.
- Es fácilmente identificable utilizando diccionarios o bien consiste en nombres propios, fechas significativas, números conocidos o variaciones simples de estas palabras.

Por otra parte, en el caso de olvido de la contraseña, algunos programas permiten recuperarla o modificarla contestando una pregunta establecida por la misma persona usuaria. De la complejidad de la respuesta a esta pregunta también depende la robustez de la contraseña.

La empresa tiene que establecer, en las normas de uso del correo electrónico, una política de contraseñas adecuada para garantizar la identificación inequívoca y personalizada de cualquier usuario.

Recomendaciones

- ✓ Establecer, para el acceso a la cuenta de correo, un mecanismo que garantice la identificación de forma inequívoca y personalizada de cualquier usuario y su autenticación mediante una contraseña fuerte.
- ✓ No crear usuarios que se identifiquen con la dirección de correo, dado que facilitaría la identidad del usuario y daría a un tercero la posibilidad de bloquear la cuenta.
- ✓ Almacenar los usuarios y las contraseñas, o cuando menos las contraseñas, de forma ininteligible, utilizando técnicas de cifrado.

- ✓ Mantener la confidencialidad del usuario y la contraseña atribuidos cuando se comunican por primera vez al usuario.
- ✓ Evitar riesgos cuando se envían las contraseñas al servidor de correo, utilizando sistemas de transmisión segura, como el cifrado.
- ✓ Establecer la periodicidad con que se tiene que modificar la contraseña, que en ningún caso tiene que ser superior a un año.
- ✓ No permitir, en caso de cambio periódico de la contraseña, que se repitan las últimas contraseñas utilizadas.
- ✓ Prohibir expresamente el uso no autorizado del correo electrónico de otros usuarios mediante el intercambio de usuarios o usuarios compartidos.
- ✓ Instalar sistemas de bloqueo en el ordenador que se puedan activar fácilmente en caso de ausencia o que obliguen al usuario a volver a introducir su contraseña después de un determinado periodo de inactividad.
- ✓ Informar a los usuarios de lo siguiente:
  - Sus obligaciones en relación con la conservación de las contraseñas y los periodos de modificación.
  - El carácter personal y no transferible de los usuarios y contraseñas.
  - Las responsabilidades en que se puede incurrir por la pérdida, alteración fraudulenta o suplantación en los sistemas de autenticación.
- ✓ Establecer un protocolo adecuado para retirar los permisos de acceso, cuando un trabajador deja de prestar servicios a la entidad.

3 Seguridad de las comunicaciones

La utilización del correo electrónico, por sí sola, no garantiza la autenticidad ni la integridad de la comunicación. Es decir, no garantiza la autenticidad de la identidad de quien aparece como emisor ni que el contenido emitido coincida con el contenido recibido. Ello puede generar problemas tanto respecto a la suplantación de la identidad como respecto a la alteración de los mensajes y archivos adjuntos.

Para garantizar la autenticidad y la integridad de las comunicaciones, se puede utilizar la firma electrónica.

❑ Firma electrónica

La firma electrónica es un conjunto de datos en forma electrónica que, consignados o asociados con otros, se pueden utilizar como medio de identificación de la persona que firma, mediante un sistema de criptografía asimétrica. Este mecanismo permite autenticar el emisor y la integridad del mensaje.

La firma electrónica se puede generar a partir de un certificado electrónico, esto es, un documento firmado electrónicamente por un prestador de servicios de certificación, que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Cada administración, con la colaboración, si procede, de la Agencia Catalana de Certificación, tiene que proveer a su personal de sistemas de firma electrónica, que pueden identificar de forma conjunta el titular del puesto de trabajo o cargo y la administración donde presta servicios.

En la web de la Autoridad Catalana de Protección de Datos, podéis encontrar información sobre cómo utilizar la firma electrónica en diferentes sistemas de correo electrónico.

Por otra parte, hay que asegurar también la confidencialidad de la información transmitida, es decir que sólo tengan acceso las personas adecuadas.

❑ Cifrado

Para garantizar la confidencialidad de las comunicaciones, se puede utilizar el cifrado.

El cifrado consiste en la transformación de un mensaje, utilizando una clave para evitar que quien no la conozca lo pueda interpretar.

Es obligatorio utilizar mecanismos de cifrado de los datos o bien cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros, en la transmisión de datos de carácter personal a través de redes públicas o redes sin hilo de comunicaciones electrónicas de datos, cuándo el tratamiento requiera la aplicación de medidas de seguridad de nivel alto:

- Datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Datos obtenidos con fines policiales sin el consentimiento de las personas afectadas.
- Datos derivados de actos de violencia de género.

En la web de la Autoridad Catalana de Protección de Datos, podéis encontrar información sobre cómo utilizar el cifrado en diferentes sistemas de correo electrónico.

El sistema de correo tiene que garantizar la seguridad de la información vinculada a su utilización. En este sentido, hay que tener en cuenta que la salida de información de carácter personal por medio del correo electrónico, ya sea en el texto del mensaje o en los ficheros adjuntos,

la tiene que autorizar el responsable del fichero o tiene que estar debidamente autorizada en el documento de seguridad.

También conviene tener en cuenta que algunas páginas web o correos electrónicos pueden incorporar *web bugs* (pequeñas imágenes incrustadas que pueden dar información sobre nuestra dirección IP y sobre nuestro acceso al correo) o hipervínculos invisibles que permiten transmitir la dirección de correo electrónico a un tercero.

La empresa tiene que preveer, en el protocolo incluido en las normas de uso del correo electrónico, que las personas trabajadoras que detecten algún tipo de incidencia, o bien duden sobre la seguridad del sistema, lo comuniquen inmediatamente al responsable de seguridad, con una breve descripción del incidente y la fecha y hora en que se haya detectado, para que se resuelva la incidencia y/o se revise el funcionamiento de su correo electrónico.

Recomendaciones

- ✓ Establecer por defecto una configuración de seguridad en los equipos y programas de correo adecuada a la naturaleza de los datos más sensibles que se prevea que se trataran.
- ✓ Proteger siempre el acceso al buzón de correo con un sistema que garantice la identificación y la autenticación, especialmente cuando se recibe en dispositivos móviles.
- ✓ Orientar las pantallas de los terminales de manera que se preserve el contenido de los mensajes respecto de terceras personas que se puedan encontrar en las dependencias donde se halle el puesto de trabajo.
- ✓ Configurar los dispositivos móviles para que se bloqueen automáticamente a fin de que, en caso de pérdida, ninguna otra persona pueda acceder a los mensajes de correo electrónico.
- ✓ Prohibir la instalación de software no autorizado por la empresa.
- ✓ Instalar software antivirus, filtros antiinundación o *anti-spam* u otros mecanismos para reducir la recepción de mensajes no solicitados.
- ✓ Requerir al proveedor que la comunicación entre el dispositivo de acceso al correo y el servidor esté cifrada.
- ✓ Pedir que se eliminen, de forma inmediata, los mensajes que puedan contener virus o *malware* o software malicioso. El borrado completo requiere eliminarlos también de la papelera de reciclaje.
- ✓ Establecer un sistema adecuado de resolución de cualquier incidencia de seguridad que se detecte en el sistema.
- ✓ Incluir en las normas de uso del correo instrucciones sobre el uso de la firma electrónica y el cifrado de los mensajes.
- ✓ Formar al personal en la utilización de los instrumentos de firma electrónica y cifrado de los mensajes.

4 Uso del correo con finalidades privadas

El desarrollo de las funciones atribuidas a muchos puestos de trabajo hace indispensable la atribución de una cuenta de correo electrónico para poder llevar a cabo de una forma eficaz las funciones encomendadas. A menudo, sin embargo, puede resultar difícil separar de una forma hermética la vida privada de las personas trabajadoras respecto de su actividad profesional. Y ello no sólo por la actuación de la persona trabajadora, sino también por necesidades de la misma empresa y porque además, la persona trabajadora no siempre puede controlar los mensajes que recibe en su cuenta de correo. Esto es especialmente evidente en el caso de dispositivos móviles o sistemas de acceso remoto establecidos, precisamente, para poder acceder a estos medios fuera del puesto de trabajo y del horario laboral.

Ello permite distinguir entre diferentes tipos de cuentas de correo, de acuerdo con su finalidad:

- **Cuenta corporativa para uso laboral:** es propiedad de la empresa o institución en la cual se presta servicios, quien determina tanto el usuario como el proveedor y el dominio, y también las finalidades y condiciones de uso a que está sometido. La atribución de esta cuenta de correo se hace por motivos estrictamente laborales.

- **Cuenta corporativa para uso privado:** la empresa puede atribuir al trabajador una cuenta de correo electrónico para uso estrictamente particular. Podrá limitar el uso, pero no controlar su contenido.

- **Cuenta privada o personal:** lo proporciona algún proveedor de servicios, sea de manera gratuita o mediante pago, o la empresa o institución en la cual se presta servicios. Este correo es de uso estrictamente personal.

La atribución de la cuenta de correo calificado como corporativo o laboral obedece a motivos estrictamente laborales. No obstante, tal como se ha expuesto, vista la dificultad en muchos casos de separar la vida privada de la actividad laboral, y a menos que la empresa establezca expresamente lo contrario, hay una cierta aceptación social respecto de la posibilidad de utilizar estos medios para finalidades privadas.

Conviene, sin embargo, que en las normas de uso del correo electrónico la empresa establezca si el uso privativo de este medio es admisible, y en qué medida (horario, volumen de los mensajes enviados o recibidos, etc.).

Cuando sea admisible una cierta utilización del correo con fines privados, una actuación diligente de la persona trabajadora permite asegurar el respeto a su privacidad. A este efecto, resulta fundamental limitar la difusión de la dirección de correo profesional a finalidades estrictamente profesionales, configurar los mensajes de forma adecuada, organizarlos y verificar periódicamente los que se tienen que eliminar.

Por otra parte, para hacer compatibles la prohibición de utilizar el correo laboral con finalidades privadas y el desarrollo de la vida privada de las personas, cuando las circunstancias lo aconsejen, puede ser recomendable atribuir no sólo una cuenta corporativa o laboral sino también una cuenta privada o personal, con el fin de evitar, o como mínimo reducir, la utilización de una misma cuenta con finalidades diversas. La atribución de este correo personal puede sustituirse por una autorización para utilizar algún sistema de correo web, con los límites que establezca la misma empresa.

Conviene también, si procede, informar a las otras personas con las que previsiblemente pueda relacionarse sobre el carácter exclusivamente profesional de las direcciones de correo electrónico (p.ej. a través de la inserción de un aviso en todos los mensajes salientes de la organización, o con un aviso en el directorio corporativo).

En cualquier caso, la asignación de una dirección de correo que no incorpore datos vinculados a una persona concreta puede facilitar que terceras personas perciban el carácter exclusivamente profesional de la cuenta de correo.

Cuando, en caso de ausencia, la continuidad del servicio requiera redireccionar los mensajes que lleguen a una determinada cuenta de correo a la cuenta de correo de otra persona trabajadora, conviene advertir con antelación suficiente a la persona afectada, para que pueda adoptar las medidas adecuadas y, si procede, advertir de este hecho a sus contactos.

Recomendaciones

- ✓ Establecer, en las normas de uso del correo, si las personas trabajadoras pueden utilizar la cuenta de correo profesional con finalidades personales.
- ✓ Admitir el uso en el ámbito laboral de un sistema de correo vía web para finalidades privadas, concertado por la misma persona interesada y con los límites de las normas de uso del correo electrónico de la empresa.

En caso que se admita la utilización de la cuenta de correo profesional con finalidades personales:

Recomendaciones

- ✓ Establecer, en las normas de uso del correo electrónico, un periodo máximo de conservación de los mensajes privados. Si las personas trabajadoras no han borrado antes los mensajes que sean innecesarios, o los han reenviado a una cuenta de correo privado, al cumplirse este plazo las personas trabajadoras tienen que borrar los mensajes de esta naturaleza.
- ✓ Establecer las normas de uso de los dispositivos móviles con acceso al correo electrónico, como teléfonos inteligentes o *smartphones* u ordenadores portátiles, fuera del horario laboral.
- ✓ Crear carpetas para almacenar los correos identificados como “privados” o “personales”. Ello se puede hacer de manera automática, mediante filtros a partir de su origen o que incluyan estas expresiones u otras preestablecidas en el asunto del mensaje, o manualmente a partir de la decisión del titular de la cuenta de correo.

5 Uso del correo con finalidades sindicales

La libertad de información es un elemento esencial del derecho fundamental a la libertad sindical. Aunque la legislación laboral no prevé expresamente, para el ejercicio de este derecho, el uso de los medios tecnológicos que la empresa pone a disposición de las personas trabajadoras para desarrollar sus funciones, los representantes de las personas trabajadoras pueden ejercer este derecho mediante el uso de las tecnologías de la información y la comunicación, siempre que esto no afecte al despliegue normal de la actividad empresarial.

No hay una previsión legal expresa de facilitar la transmisión de información sindical a los trabajadores, afiliados o no, por medio de un sistema de correo electrónico a cargo de la empresa. No obstante, si la empresa dispone de este medio, los representantes de las personas trabajadoras pueden utilizarlo para transmitir noticias de interés sindical a sus afiliados y al resto de trabajadores de la empresa, de acuerdo con las normas de uso del correo electrónico de la empresa.

En cualquier caso, el uso del correo electrónico proporcionado por la empresa por parte de los representantes de las personas trabajadoras con esta finalidad está sujeto, de acuerdo con la doctrina constitucional establecida, a una serie de límites:

- No se puede excluir la utilización del correo electrónico con esta finalidad en términos absolutos.
- La comunicación no tiene que perturbar la actividad normal de la empresa.
- Su uso no puede comportar gravámenes o costes adicionales para la empresa.

Con esta misma finalidad, los representantes sindicales también pueden utilizar, sin consentimiento de las personas interesadas, las direcciones que figuren en el directorio de la empresa.

En cualquier caso, los trabajadores pueden ejercer su derecho de oposición a la utilización de su dirección de correo electrónico con esta finalidad delante del responsable del fichero.

Recomendaciones

- ✓ Autorizar el uso del correo electrónico como instrumento de comunicación e información entre sindicatos y trabajadores, con garantía de inviolabilidad de las comunicaciones de acuerdo con el marco legal vigente, siempre que la actividad y las características generales de la empresa lo permitan. No obstante, conviene valorar la posibilidad de difundir la información sindical entre las personas trabajadoras, mediante sistemas que permitan hacerlo sin necesidad de recoger el dato del correo de las personas trabajadoras, como por ejemplo:
- ✓ Utilizar listas de distribución que permitan que el sindicato remita la información sin acceso a los datos.
- ✓ Poner una ventanilla de información sindical a disposición de las personas trabajadoras, en la intranet corporativa.
- ✓ Establecer un procedimiento fácil para el ejercicio, delante del sindicato y/o el responsable del fichero, del derecho de oposición a la utilización de la dirección electrónica con esta finalidad.
- ✓ Informar a los trabajadores de la posibilidad de ejercer este derecho, en el momento que se faciliten los datos a los representantes de los trabajadores, a menos que ya se les haya informado antes. Ello sin perjuicio que el representante sindical también informe debidamente a los trabajadores.

III. El acceso al correo electrónico por parte de la empresa

Las consideraciones contenidas en este apartado se refieren no sólo a las cuentas de correo en las cuales las normas de uso de la empresa admiten un cierto uso privado, sino también respecto de las cuentas de correo en relación con las cuales se establezca un uso exclusivamente profesional, dado que con independencia del uso que haga el mismo trabajador, éste no siempre puede evitar el uso que de las mismas hagan terceras personas para remitirle mensajes de carácter personal.

La empresa sólo puede acceder a las cuentas de correo electrónico corporativo facilitadas a sus trabajadores cuando el acceso esté justificado y no haya ningún otro mecanismo que permita alcanzar el objetivo perseguido sin necesidad de acceder a las mismas.

El medio y el alcance del control tiene que ser proporcionado a la finalidad que se persiga. Por eso, si es posible, se tiene que limitar a los datos sobre el emisor y el receptor, la hora de la comunicación y otros datos como el número de mensajes enviados, el volumen de información o el tipo de archivos que se haya adjuntado u otros sistemas de análisis automatizado de los mensajes entrantes y salientes que no analicen su contenido. Sólo si esta información no es suficiente para alcanzar la finalidad perseguida, se podrá acceder al contenido de los mensajes siempre que se cumplan las garantías apropiadas, evitando entrar en los mensajes que se puedan identificar como privados. En caso de que un mensaje de esta naturaleza se abra por error, hay que cerrarlo tan pronto como se pueda constatar su naturaleza privada.

Este acceso se debe llevar a cabo de acuerdo con las normas de uso del correo electrónico que apruebe la empresa, las cuales deben advertir sobre los mecanismos de control del uso de las tecnologías que puedan afectar a la privacidad de las personas, de las consecuencias que se pueden derivar del control y de las garantías para las personas trabajadoras, en especial su derecho a ser informadas.

Se tiene que informar tanto al administrador del sistema como al resto de personas que intervengan en las operaciones de control de sus deberes y obligaciones en materia de seguridad, y en especial del deber de secreto. Sin perjuicio de la obligación general de secreto que se deriva de la normativa de protección de datos, puede ser conveniente hacer firmar a las personas que intervienen en estas operaciones un compromiso de confidencialidad respecto de los datos a los que tengan acceso.

El acceso que se lleve a cabo en cualquiera de los supuestos descritos tiene que quedar debidamente reflejado en el registro de incidencias.

Las personas trabajadoras pueden ejercer sus derechos de acceso, rectificación, cancelación y oposición respecto de la información que haya obtenido la empresa a través de las medidas de control implantadas.

El acceso se tiene que limitar a la información que resulte indispensable para alcanzar alguno de los objetivos siguientes:

1 Acceso para realizar tareas de mantenimiento del correo electrónico

El acceso a las cuentas de correo electrónico corporativo para las tareas de mantenimiento, el soporte técnico o la seguridad del sistema no tiene que comportar el acceso al contenido de los mensajes. Se puede llevar a cabo teniendo en cuenta:

- ❑ Estas operaciones sólo las puede hacer el personal autorizado por el responsable de seguridad.
- ❑ Se tiene que informar a las personas trabajadoras afectadas sobre las tareas que se deberán llevar a cabo y las personas que las ejecutarán, como también de la posibilidad de estar presentes durante el acceso.
- ❑ Una vez finalizadas las tareas de mantenimiento o de soporte técnico, conviene elaborar un informe de las tareas hechas y, si se ha detectado alguna anomalía, anotarla en el registro de incidencias y comunicarla al órgano competente.

2 Acceso para garantizar la continuidad de la actividad en ausencia de la persona trabajadora (vacaciones, enfermedad, etc.)

La ausencia de un trabajador, especialmente si es de larga duración, puede comportar problemas para la continuidad de la actividad normal de la empresa, si no se puede acceder a una determinada cuenta de correo. Por ello es conveniente, si es posible, planificar las medidas que se adoptarán para garantizar la continuidad durante la ausencia (p. ej. la persona trabajadora puede eliminar o trasladar todos los mensajes personales y autorizar el acceso a otro trabajador, adoptando los cambios pertinentes, tanto en el inicio como en el fin del periodo, respecto al cambio de las contraseñas).

Si ello no es posible, hay que tener en cuenta:

- ❑ El órgano superior de la persona trabajadora ausente tiene que valorar de forma motivada la necesidad de la intervención para la continuidad del servicio.
- ❑ El acceso a la cuenta de correo electrónico se tiene que comunicar a la persona trabajadora con suficiente antelación. Si no fuera posible esta comunicación previa, se tiene que hacer posteriormente, tan pronto como sea posible.
- ❑ Conviene acceder a ella bajo la supervisión del órgano superior de la persona trabajadora y, en el caso que se le haya podido comunicar, con su asistencia o de la persona que designe, si lo desea.
- ❑ No se puede acceder, por este motivo, a los mensajes que se puedan identificar claramente como privados o personales.

3 Acceso cuando haya indicios de un posible mal uso

Por razones de seguridad, la empresa puede monitorizar el tráfico de correo electrónico (número de mensajes, volumen de mensajes o ficheros adjuntos etc.), sin entrar a analizar su contenido. Esta monitorización puede ser sistemática o aleatoria, sin que en ningún caso pueda ser discriminatoria.

Si hay indicios de un mal uso del correo por parte de la persona trabajadora, por incumplir las normas que haya aprobado la empresa, se tiene que poner en conocimiento de la persona trabajadora, a menos que esto pueda obstaculizar las investigaciones que procedan. Cuando este mal uso pueda ser constitutivo de delito o falta, se ha de comunicar al ministerio fiscal. Cualquiera de estos casos puede dar lugar a una información reservada o a un procedimiento disciplinario, en cuyo seno se pueden adoptar las medidas que estén al alcance para solucionar el problema, que pueden incluir el bloqueo de los mensajes.

En este acceso, que tiene que ser proporcionado al tipo de riesgo que se pueda derivar del mal uso del correo para la empresa o terceras personas, conviene tener en cuenta:

- ❑ El acceso lo tiene que llevar a cabo la persona designada por el responsable de seguridad, en presencia de la persona trabajadora o, si ello no es posible, del representante del personal y de la persona instructora o inspectora.
- ❑ Una vez se ha accedido, conviene elaborar un informe de las actuaciones realizadas y de los resultados obtenidos e incorporarlo, si procede, al expediente correspondiente.

4 Cese de la relación laboral de la persona trabajadora con la empresa.

Cuando una persona trabajadora deje de prestar servicios en la empresa, el órgano competente en materia de gestión de personal tiene que comunicarlo inmediatamente al responsable de seguridad para que se inutilicen los códigos de usuario y las contraseñas del trabajador y, si procede, se incluya un mensaje automático de respuesta para el correo entrante que indique la nueva dirección a la cual se pueden dirigir los mensajes por razones profesionales.

La empresa tiene que facilitar a la persona trabajadora la obtención de los mensajes privados de la cuenta de correo, siempre que no superen el periodo máximo de conservación establecido en las normas de uso del correo para los mensajes de esta naturaleza. En este caso, se accederá a los mismos en presencia de la persona trabajadora, con el fin de identificar los mensajes de carácter exclusivamente personal.

Los mensajes se pueden borrar o transferir a otra cuenta de correo, una vez haya transcurrido el plazo otorgado a la persona trabajadora sin que haya manifestado la intención de llevarse o destruir los mensajes privados que en ella se contenían.

En caso de defunción de la persona trabajadora, los mensajes personales se pueden borrar, sin perjuicio de que se mantengan, debidamente bloqueados, si las circunstancias lo aconsejan.